

Financial Management Service

Privacy Impact Assessment

Name of Project: Background Information Case Management

System Project's Unique ID: Pay.gov

Data in the System¹

1. In general terms, what information is to be used in the system?

The Financial Management Service's (FMS) transaction portal Pay.gov system is available for Federal agencies to use in processing forms, bill, authentication decisions, collections, and for obtaining information about those transactions. The information concerns Federal agency transactions involving the public, both consumers and businesses.

Form and billing information can cover any of the items that appear on a Federal agency form or bill, if processed by Pay.gov.

Collection and payment information can include transaction amounts, methods, financial account information, names, addresses, Taxpayer Identification Numbers, agency deposit and debit ticket numbers, Treasury and agency account symbols, agency location codes, Treasury and agency transaction identifiers, transaction dates, and transaction statuses. System coverage of collection information currently is limited to certain electronic transactions handled by Pay.gov, but this coverage may eventually expand to include other information, including paper lockbox transactions. System coverage of payment information currently is limited to a handful of agency records, including Social Security Administration payments, Internal Revenue Service payments, and payments to Federal employees, but will include other methods in the future. With the exception of certain credit card credits, Pay.gov does not process payments but rather uses this information only for authentication purposes.

Authentication information can include the above as it relates to specific persons, as well as telephone numbers, driver's license numbers, dates of birth, employer information, and usernames and passwords. It will include the end-user's roles for particular electronic resources (Web pages or applications) as well as a handful of agency-specific "extension" fields that limit the scope of particular roles, can be used for pre-population of forms, or the handling of application-level business rules.

¹ This document is based upon the questions posed in the "Internal Revenue Service Model Information Technology Privacy Impact Assessment" (version 1.3, December 17, 1996), named as a best practice by the Federal Chief Information Officer's Council <<http://cio.gov>> on February 25, 2000.

2. What are the sources of the information in the system?

a. What FMS files and databases are used?

In addition to credit card credits processed by Pay.gov, Pay.gov obtains payments information from daily files received from Treasury agents that are fed into a larger Treasury payments database, named PACER. Pay.gov obtains collection information from the Treasury agents and contractors that process collections. Pay.gov authentication administrators will provide some authentication information.

b. What Federal agencies are providing data into the system?

In order to populate bills, Pay.gov obtains billing information from Federal agencies that choose to use the service, but some of this information may be changed by end-users at the time of transaction to the extent the agency allows. The particular Federal agencies that provide data will change and accumulate over time.

c. What state and local agencies are providing data into the system?

No state and local agencies are directly providing data, but some information from third party databases used by Pay.gov's verification engine may include information originally in state databases, such as driver's license numbers.

d. From what other third party sources will data be collected?

Some of the collection information will result from processing by collection networks run by third parties, particularly the Automated Clearing House and credit card networks. The verification engine will require input from third party databases, in addition to the internal payment and collection records noted above, to judge the accuracy of information provided by end-users. Information obtained from third party databases will be maintained only for a short time in audit logs.

e. What data will be obtained from the end-user?

Pay.gov obtains forms information and edited bill information from end-users. Pay.gov obtains authentication information from end-users, including self-selected usernames and passwords.

3.

a. How will data collected from sources be verified for accuracy?

Form and billing information provided by end-users is subject to error checking to ensure that the information is accurate. This error checking primarily occurs on the end-user's browser to ensure the validity of the information, according to rules set out by the agency responsible for the bill or form. Billing information provided by agencies is checked for accuracy by the agency.

Payment information provided by Treasury agents is checked for accuracy by the agents. Pay.gov also applies certain edits prescribed by PACER to ensure that the information is properly formatted.

Collection information provided by end-users is subject to browser-based and server-based error checking to ensure that the information is accurate. These edits include eliminating the possibility of zero-dollar transactions and the scheduling of collection dates in the past. In addition, financial account information is subject to edits to ensure that, for Automated Clearing House debits, that the routing number is valid and that the account structure is reasonable and for credit card collections, that the card is valid.

Authentication information provided by end-users is compared with information contained in Pay.gov and 3rd party databases (Government and commercial) to ensure that the information is accurate. Multiple databases are used because of the possibility that any one database is inaccurate in its information. A Pay.gov “verification engine” will consolidate the results from the various database comparisons to provide confidence levels associated with each data element supplied by the end-user, as well as overall. If these confidence levels meet Pay.gov or another agency’s standards, the end-user is authenticated and authorized to use those services that required this type of “ad hoc,” time-of-transaction, knowledge-based authentication.

b. How will the data be checked for completeness?

Form and billing information provided by end-users is subject to error checking to ensure the completeness of the information. This error checking primarily occurs on the end-user’s browser to ensure the validity of the information, according to rules set out by the agency responsible for the bill or form. Incomplete information will be rejected. Billing information provided by agencies is checked for completeness by the agency and is subject to checks by Pay.gov to ensure completeness. If incomplete, the information will be rejected.

Payment information provided by Treasury agents is checked for completeness by the agents. Pay.gov also applies certain edits prescribed by PACER to ensure that the information is properly formatted.

Collection information provided by end-users is subject to browser-based and server-based error checking to ensure that the information is complete. These edits include ensuring that all necessary fields are provided. Information processed as files by agents will have header information that summarizes the transactions contained in the file; if the file information differs from the header, an exception is thrown. Additional proofing (internal checking of information) and balancing (checking information against external sources) is planned for future releases.

Authentication information provided by end-users is subject to browser-based and server-based error checking to ensure that the information is complete. The verification engine will invoke multiple databases to mitigate the possibility that any one database is incomplete in its coverage.

c. Is the data current?

All information provided by end-users, Treasury agents and contractors is presumed to be current when first provided, except for certain authentication information obtained from third party databases. This information could be out of date. In addition, when used for authentication, payment and collection information from Treasury databases could be out of date. Due to the limitations of knowledge-based authentication systems (accuracy, completeness, timeliness), multiple databases are used to provide the best chance of a true result.

Access to the Data

1. Who will have access to the data?

Bill (including bills saved after editing) and saved form information will be made available to end-users; to the extent it involves their own transactions. An agency will have access to submitted bill and form information; to the extent it involves the agency. An agency will also be able to check the status of bills, as will Pay.gov customer service.

Collection information will be made available to end-users; to the extent it involves their own transactions. An agency will have access to collection information; to the extent it involves the agency, as Pay.gov customer service. Collection information also will be available to the depository that processes the collection. By necessity, collection information must be shared with external networks such as the Automated Clearing House network and credit card network.

Authentication information will be made available to end-users to the extent it involves profile information associated with a Pay.gov username and password. This information will be made available to an agency if the end-user so agrees. It will be available to Pay.gov authentication administrator and to customer service. It will be available to an agency authentication administrator and a business authentication administrator if that administrator created the profile.

Responses from the verification engine will not be made available to end-users (except on a yes/no basis when used for limited, controlled “live demo” purposes) but will be made available to an agency if the end-user so agrees. By necessity, the information must also be shared with third parties that operate the databases that provide responses used by the verification engine.

The above will be available to Pay.gov program management and database administrators. Information also will be made available to other program representatives, including developers, as determined by the Pay.gov program manager or the Pay.gov information system security officer as needed to investigate improvements, security breaches, or possible error resolution.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to data by an end-user requires that an end-user be authenticated using a Pay.gov username and password. If it is for viewing form or bill information, the end-user also may be authenticated by an agency and handed to Pay.gov.

Access to data by an agency—either a representative or an agency system—requires authentication of the agency, either by Pay.gov username and password or by digital certificate (in the case of an agency system).

Access to data by Pay.gov program management and customer service requires a Pay.gov username and password. Access to databases by Pay.gov database administrators and to audit logs by Pay.gov system administrators requires two-factor authentication issued by the Treasury Web Application Infrastructure. Access to profile data by a Pay.gov, business, or agency authentication administrator requires that the person be authenticated using a Pay.gov username and password. As set out in a standard operating procedure, Pay.gov authentication administrators must apply for their Pay.gov username and password on an approved paper form and must grant usernames and passwords to others only upon having received an approved paper form.

All database administrators, Pay.gov management representatives, Pay.gov customer service representatives, and Pay.gov authentication administrators will have to sign Privacy Act non-disclosure agreements prescribed by the Treasury Security Manual if they are not FMS or fiscal agent² employees. All agents (other than fiscal agents) and contractors whose employees may access Privacy Act data have agreements that include Privacy Act provisions. These and other persons designated by the Pay.gov information systems security officer (a FMS employee) as “high risk” must undergo a background investigation and credit check. Agents (other than fiscal agents) are required to provide training on a quarterly basis to employees and contractors. Certain database fields are encrypted to further ensure protection against unauthorized access.

By necessity, certain information must flow to third party systems, such as collection information that is processed by Automated Clearing House and credit card networks. This information is subject to the same protections as other information that flows through those networks. Authentication information also is sent to third party database providers to obtain responses that can be used by the verification engine. However, by agreement, the third party database provider is not to retain any delivered information it did not already own.

All online access is conditioned upon agreement to the language contained on the “Notices and agreement” page, which includes rules of behavior. All information that moves between Pay.gov and any other entity is either protected using hardware-based, version-3 only, 128-bit Secure Socket Layer encryption or delivered over dedicated lines.

3. Will users have access to all data on the system or will access be restricted?

End-users will have Web-based access to see only their bills, saved (edited) bills, saved forms, and status of collections regarding submitted transactions, if authenticated by a Pay.gov

² Fiscal agents (Federal Reserve Banks) are waived from certain security requirements because of the strong internal controls followed by Federal Reserve Banks, as reflected in public audit results for those banks.

username and password or through by agency authentication. End-users also have the ability to change profile information associated with their Pay.gov username and password.

Agency access depends upon the agency user. An agency will receive a file of electronic (but non-Web) details of forms, bills, and collections, and (for applications hosted on the agency site) authentication.

Depository access entails the ability to receive detailed collection information needed to process collections, which by necessity entails use of collection networks, and provides replies on the status of collections. Depository representatives also will be able to receive Web-based detail information regarding individual collections transactions that track to the depository.

Third parties will receive details of collections necessary to process collections and provide responses. The database will receive details necessary to provide responses back to the verification engine. Business authentication administrators will have the same access as agency administrators, insofar as that businesses end-users for the agency's resources are concerned.

4. What controls are in place to prevent misuse (i.e., browsing) of data by those having access?

Pay.gov security requirements and the "Notice and agreement" page forbid browsing by personnel working for the Pay.gov project. In addition, only database administrators will have the ability to search records by an end-user's name or Taxpayer Identification Number. All other personnel working for the Pay.gov project will have the ability to search only on non-personally identifying fields, with the exception of financial account information (account and card numbers). Agreements with the third party database providers require that the providers do not retain data elements not already possessed by the provider and include audit provisions.

5.

a. Do other systems share data or have access to data in this system? Who will be responsible for protecting the privacy rights of the users and employees affected by the interface?

The above addresses the systems that share data or have access to data. The Pay.gov program manager and information system security officer will have responsibility for ensuring compliance.

6.

- a. **Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)? How will the data be used by the agency? Who is responsible for ensuring proper use of the data? How will the system ensure that agencies only get the information they are entitled to under 26 § U.S.C. 6103?**

The above addresses the agencies that share data or have access to data.

Form, bill, and collection information is used by the agency as it chooses for its internal operations. Authentication information is shared with an agency when an agency has an application on its own site that requires authentication information. It may not be used for other purposes, such as credit checks on the end-user.

The Pay.gov program manager and information system security officer will have responsibility for ensuring compliance.

Insofar as ensuring that agencies only get the information to which are entitled, the form, bill, and collection information is needed for the agency's programs. Although the collection information is also Pay.gov records, the information is otherwise the agency's own information; Pay.gov is a pass-thru. Authentication information is provided only with the consent of the end-user, except for profile information created by agency authentication administrators.

In some respects, the authentication information that is shared from the verification engine is not a disclosure, let alone one under 26 § U.S.C. 6103. The information shared with the agency often reflects a consolidation of results obtained through the comparison of end-user provided data against multiple databases, some of which are not Governmental databases. Other than successful confidence percentages, no additional data elements are passed to the agency other than that which was obtained from the end-user. Some confidence percentages can result from the payments database, which includes payments of IRS tax refunds, among other sources. However, there is no way to determine which payments are IRS refunds and which are payments from other agencies. Finally, sharing of detailed results with agencies will be only with the consent of the end-user, which is a stated exception to both the Privacy Act and 26 U.S.C. § 6103.

Attributes of the Data

- 1. Is the use of information both relevant and necessary to the purpose for which the system is being designed?**

Form and bill information is set out by the agency; Pay.gov simply facilitates agency programs in this regard. Collection information includes only that which is necessary for collection networks to process collections. Authentication information includes a wide range of information when used for knowledge-based authentication. Pay.gov authentication credentials also include a wide range of values, but use of this data facilitates agency program needs, simplifies

completion of form, bill, and collection transactions, and in any event, end-users are able to edit many profile fields.

2.

a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

The verification engine will develop confidence percentages based upon the consolidation of query results posed to multiple databases. Pay.gov will not retain these confidence percentages except in audit logs. Pay.gov also may reformat certain financial account information to ensure that it can be processed. Otherwise, Pay.gov will not derive new data or create previously unavailable data about an individual through aggregation.

b. Will the data be placed in the individual's record?

No new data or create previously unavailable data about an individual created through aggregation will be placed in an end-user's record.

c. Can the system make determinations about users or employees that would not be possible without the new data?

The verification engine requires consolidated results to ensure the best chance of a true result. Certain Automated Clearing House transactions would be impossible without reformatting of end-user data.

d. How will the new data be verified for relevance and accuracy?

The databases used by the verification engine are subject to review to ensure that they provide relevant, accurate, and complete information, and the verification engine accounts for imperfections between databases. The system used to reformat collection information is an off-the-shelf system used by major financial institutions; furthermore, if there are problems with the data, the data will trigger returns when submitted for collection.

3.

a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Consolidated data is maintained only in audit logs, which are available only to system administrators with two-factor authentication issued by the Treasury Web Application Infrastructure. Information also will be made available to other program representatives, including developers, as determined by the Pay.gov program manager or the Pay.gov information system security officer as needed to investigate improvements, security breaches, or possible error resolution. However, all access is subject to the same restraints as set out above for non-consolidated data.

b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Pay.gov consolidates several processes:

- Collections
 - ❑ Automated Clearing House debit
 - ❑ Credit cards
 - ❑ Digital cash
 - ❑ Automated Clearing House credits (initiated offline)
 - ❑ Fedwire (initiated offline)
- Forms and bills
- Authentication
 - ❑ Ad hoc authentication
 - ❑ Agency authentication
 - ❑ Pay.gov usernames and passwords
 - Issued after ad hoc authentication
 - Issued after entry of information by:
 - Pay.gov authentication administrator
 - Agency authentication administrator
 - Business administrator
- Reporting
 - ❑ Electronic (non-Web) to agency systems
 - ❑ Web-based to reporting analysts

The controls for these processes are set out above.

4. What are the potential effects on the due process rights of users of consolidation and linkage of files and systems, derivation of data, accelerated information processing and decision making, and use of new technologies?

The verification engine touches upon each of the four categories listed in the above question. It consolidates query results from multiple databases, deriving confidence percentages as a result. It allows for instant decisions as to whether to allow transaction processing. In some instances, it can be used to grant or deny access to an electronic resource. There is a risk of “false negatives”; that is, persons who are wrongly denied access. There also is a risk of “false positives”; that is, persons who are wrongly granted access.

How are the effects/risks to be mitigated?

In order to protect end-user’s due process rights, Pay.gov has placed certain limits on the use of the verification engine. First, it will only verify information provided by the end-user. It will not be available for general queries that were not submitted by an end-user. Second, the verification engine can only be used to grant access to the sought-after resource; it cannot be used to deny access. Finally, because FMS systems are used in the authentication process, the agency will have to justify the reasonableness of the confidence percentages selected by the agency, in light of the underlying risk of the transaction.

Maintenance of Administrative Controls

1.

a. Explain how the system and its use will ensure equitable treatment of the public.

Pay.gov will consider public policy reasons in determining which applications to first enable. The verification engine will not perform credit checks on individuals to determine whether to authenticate someone, which would have a disproportionate impact on the poor.

b. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

Eventually, Pay.gov will operate in two locations, but these sites will be geographically load-balanced mirrors of one another, to ensure that data does not fall out of sync.

c. Explain any possibility of disparate treatment of individuals or groups.

Pay.gov requires Web access, which is not available to all, especially the poor, although Pay.gov anticipates at some point providing touch-tone telephone access as well.

a. What are the retention periods of data in this system?

Pay.gov’s record retention periods are still being determined.

b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?

Pay.gov's record retention procedures are still being determined.

2.

a. How does the use of this technology affect the public's privacy?

As noted above, the verification engine is a tool that is appropriate in some, but not all, situations. Used properly, it can enhance the public's privacy by giving greater electronic access to information and services. Used improperly, it can wrongly deny access to electronic services or allow another to wrongly access electronic services while impersonating someone else.

3.

a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The verification engine and site monitoring software can be used to determine information relating to persons. The verification engine, described above, confirms information from end-users, including the end-user's name and address. It does not track or monitor individuals.

Pay.gov will not use persistent "cookies", which are files placed on a visitor's hard drive that allows the Web site to monitor the individual's use of the site. Use of cookies are a common practice by many commercial and government Web sites in order to customize the user's visits to the site, however, the FMS will not monitor an individual's activities on Pay.gov by embedding persistent cookies on end-users' hard drives.

Except for authorized law enforcement investigations, Pay.gov does not use this automatically gathered information to identify individual users or their usage habits.

b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

Pay.gov will not monitor groups.

4.

a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.

Pay.gov will operate under the FMS' system of records entitled, "Revenue Collection Records – Treasury/FMS .017." This is a new systems of record currently in the clearance process.

